

**UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

RICHARD TEAGUE, on behalf of  
himself individually and on behalf of  
all others similarly situated,

Plaintiff,

v.

AGC AMERICA, INC.

Defendant.

Case No.: \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**DEMAND FOR A JURY TRIAL**

Plaintiff Richard Teague (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant AGC America, Inc. (“AGC” or “Defendant”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigation, and upon information and belief as to all other matters, as follows:

**NATURE OF THE ACTION**

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personal information of Defendant’s current and former employees and prospective employees, including, but not limited to, first and last names, Social Security numbers, driver’s license numbers, financial account information associated with direct deposits, passports, payment card numbers,

company network login credentials (“personally identifiable information” or “PII”) and health insurance information, which is protected health information (“PHI”, and collectively with PII, “Private Information”) as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

2. Boasting “over 27,000 member firms,” AGC is the “leading association for the construction industry.”<sup>1</sup>

3. The Private Information compromised in the Data Breach was targeted and exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals.

4. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injury in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant’s possession and is subject to further

---

<sup>1</sup> <https://www.agc.org/>

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its employees' Private Information from a foreseeable and preventable cyber-attack.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud (including the fraud suffered by Plaintiff described below), and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and continuing risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct.

### **PARTIES**

16. Plaintiff Richard Teague is and has been, at all relevant times, a resident and citizen of Quakertown, Pennsylvania.

17. Defendant AGC America, Inc. is a Delaware corporation with its principal place of business located in Alpharetta, Georgia.

### **JURISDICTION AND VENUE**

18. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

19. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

20. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

### **FACTUAL ALLEGATIONS**

#### ***Defendant's Business***

21. Boasting “over 27,000 member firms,” AGC is the “leading association for the construction industry.”<sup>2</sup>

---

<sup>2</sup> <https://www.agc.org/>

22. Plaintiff and Class Members are current and former employees at Defendant.

23. In order to apply to be an employee or obtain certain employment-related benefits at Defendant, Plaintiff and Class Members were required to provide sensitive and confidential Private Information, including their names, Social Security numbers, and other sensitive information.

24. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiff and Class Members.

25. Upon information and belief, in the course of collecting Private Information from employees, including Plaintiff, Defendant promised to provide confidentiality and adequate security for employee data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

26. Indeed, Defendant provides on its website that: “[t]his site and the servers that store collected information have industry–standard security measures in place to protect against the loss, misuse, and alteration of the information under AGC's control.”<sup>3</sup>

27. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant

---

<sup>3</sup> <https://www.agc.org/privacy-policy>

would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

29. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep employees' Private Information safe and confidential.

30. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

31. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required



submission of Private Information, Defendant could not perform the services it provides.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

### ***The Data Breach***

33. On or about February 12, 2024, Defendant sent Plaintiff and other victims of the Data Breach an untitled letter (the "Notice Letter"), informing them that:

**What Happened:** On December 14, 2023, we detected an incident that impacted the availability and functionality of our computer network. After discovering the incident, we took measures to secure our network, began an investigation, and reported the incident to law enforcement. Through our investigation, we determined that, between December 12, 2023, and December 17, 2023, an unauthorized actor accessed and acquired certain files contained on our network.

**What Information Was Involved:** Our review of the files that may have been involved identified documents that contained your name, and one or more of the following: Social Security number, driver's license number, financial account information associated with direct deposit, passport, payment card number, company network login credentials, and limited health insurance plan enrollment information for current and former health insurance plan participants.<sup>4</sup>

---

<sup>4</sup> <https://apps.web.maine.gov/online/aeviewer/ME/40/2f090dbf-dda8-44b0-90f3-2098bfce9f68.shtml>

34. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

35. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

37. The attacker accessed and acquired files in Defendant’s computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their names, Social Security numbers, and other sensitive information. Plaintiff’s and Class Members’ Private Information was accessed and stolen in the Data Breach.

38. Plaintiff further believes that his Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

***Data Breaches Are Preventable***

39. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”<sup>5</sup>

40. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

---

<sup>5</sup> See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Aug. 23, 2021).

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>6</sup>

---

<sup>6</sup> *Id.* at 3-4.

41. To prevent and detect cyber-attacks or ransomware attacks, AGC could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection

- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].<sup>7</sup>

42. Given that Defendant was storing the sensitive Private Information of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

43. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of more than 20,000 current and former employees,<sup>8</sup> including that of Plaintiff and Class Members.

***Defendant Acquires, Collects, And Stores Employees' Private Information***

44. As a condition of becoming an employee at Defendant, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Defendant.

45. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection

---

<sup>7</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

<sup>8</sup> According to the breach report submitted to the Office of the Maine Attorney General, 20,415 persons were impacted in the Data Breach. *See* <https://apps.web.maine.gov/online/aeviewer/ME/40/2f090dbf-dda8-44b0-90f3-2098bfce9f68.shtml>

of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its business services.

46. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

47. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

48. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

49. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

50. Indeed, Defendant provides on its website that: "[t]his site and the servers that store collected information have industry-standard security measures in

place to protect against the loss, misuse, and alteration of the information under AGC's control.”<sup>9</sup>

***Defendant Knew, Or Should Have Known, of the Risk Because Employers In Possession Of Private Information Are Susceptible To Cyber Attacks***

51. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

52. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting employers that collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

53. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).<sup>10</sup> The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).<sup>11</sup>

---

<sup>9</sup> <https://www.agc.org/privacy-policy>

<sup>10</sup> <https://www.idtheftcenter.org/publication/2023-data-breach-report/>

<sup>11</sup> *Id.*



54. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

55. Additionally, as companies became more dependent on computer systems to run their business,<sup>12</sup> *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.<sup>13</sup>

56. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

---

<sup>12</sup><https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

<sup>13</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

57. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

58. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>14</sup>

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to more than twenty thousand individuals’ detailed, Private Information, and, thus, the significant

---

<sup>14</sup>[https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=consumerprotection](https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection) (last accessed Oct. 17, 2022).

number of individuals who would be harmed by the exposure of the unencrypted data.

61. In the Notice Letter, Defendant makes an offer to provide identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' Private Information. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

62. Defendant's offering of credit and identity monitoring demonstrates that Plaintiff and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

64. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

65. As an employer in possession of its current and former employees' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

***Value of Personally Identifying Information***

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>15</sup> The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."<sup>16</sup>

67. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web

---

<sup>15</sup> 17 C.F.R. § 248.201 (2013).

<sup>16</sup> *Id.*

pricing for stolen identity credentials.<sup>17</sup> For example, Personal Information can be sold at a price ranging from \$40 to \$200.<sup>18</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>19</sup>

68. For example, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>20</sup>

---

<sup>17</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 17, 2022).

<sup>18</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 17, 2022).

<sup>19</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 17, 2022).

<sup>20</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

69. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

70. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."<sup>21</sup>

71. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."<sup>22</sup>

---

<sup>21</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Oct. 17, 2022).

<sup>22</sup> *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, available at: <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658> (last visited July 31, 2023).

72. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.”<sup>23</sup>

73. According to national credit bureau Experian:

A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

74. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation.”<sup>24</sup>

However, this is not the case. As cybersecurity experts point out:

“It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.”<sup>25</sup>

---

<sup>23</sup> <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658> (last visited on Feb. 21, 2023).

<sup>24</sup> <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/> (last visited on Feb. 21, 2023).

<sup>25</sup> *Id.*

75. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.<sup>26</sup>

76. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>27</sup>

77. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.*, patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a “cyber black market” exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

---

<sup>26</sup> *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at: <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited on Feb. 21, 2023).

<sup>27</sup> *Medical I.D. Theft*, EFraudPrevention <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected>. (last visited Nov. 6, 2023).



Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

78. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.<sup>28</sup> Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.<sup>29</sup> In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.<sup>30</sup>

79. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.<sup>31</sup>

80. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions

---

<sup>28</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last accessed July 24, 2023).

<sup>29</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed July 24, 2023).

<sup>30</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/> (last accessed July 24, 2023).

<sup>31</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021)

and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities.”<sup>32</sup>

81. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.<sup>33</sup> Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.<sup>34</sup>

82. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change— i.e., Social Security numbers and names. Because the information compromised in the Data

---

<sup>32</sup> Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last accessed July 24, 2023).

<sup>33</sup> See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July 24, 2023).

<sup>34</sup> *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-know-about-them-and-what-to-do-after-one/> (last accessed July 24, 2023).

Breach is immutable, Plaintiff and Class Members are at risk of identity theft and fraud for the remainder of their lives.

83. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>35</sup>

84. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

85. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result,

---

<sup>35</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Oct. 17, 2022).

studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>36</sup>

86. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

***Defendant Fails To Comply With FTC Guidelines***

87. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

88. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand

---

<sup>36</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).

their network's vulnerabilities; and implement policies to correct any security problems.<sup>37</sup>

89. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>38</sup>

90. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data as an unfair act or practice prohibited by Section 5 of the

---

<sup>37</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Oct. 17, 2022).

<sup>38</sup> *Id.*

Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

92. These FTC enforcement actions include actions against employers, like Defendant.

93. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

94. Defendant failed to properly implement basic data security practices.

95. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

96. Upon information and belief, AGC was at all times fully aware of its obligation to protect the Private Information of its employees, AGC was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature

and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

***Defendant Fails To Comply With Industry Standards***

97. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

98. Several best practices have been identified that, at a minimum, should be implemented by employers in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. AGC failed to follow these industry best practices, including a failure to implement multi-factor authentication.

99. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible

communication system; training staff regarding critical points. AGC failed to follow these cybersecurity best practices, including failure to train staff.

100. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. These foregoing frameworks are existing and applicable industry standards for employers' caretaking of employees' Private Information and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

### ***Common Injuries & Damages***

102. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy;



(b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; and € the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as AGC fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

***Data Breaches Increase Victims' Risk Of Identity Theft***

103. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

104. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

105. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

106. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

107. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.<sup>39</sup>

108. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

109. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to

---

<sup>39</sup> "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance->](<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>) (last visited on May 26, 2023).

Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

110. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

111. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

112. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

***Loss Of Time To Mitigate Risk Of Identity Theft & Fraud***

113. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps

and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

114. Thus, due to the actual and imminent risk of identity theft, Defendant in its Notice Letter, instructs Plaintiff and Class Members to take the following measures to protect themselves: “be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.”<sup>40</sup>

115. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach and signing up for the credit monitoring and identity theft protection services offered by Defendant.

116. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO

---

<sup>40</sup> Notice Letter.

Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>41</sup>

117. Plaintiff’s mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>42</sup>

118. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>[4]</sup>

---

<sup>41</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

<sup>42</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

### ***Diminution of Value of Private Information***

119. PII and PHI are valuable property rights.<sup>43</sup> Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

120. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.<sup>44</sup>

121. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>45</sup> In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>46,47</sup> Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>48</sup>

---

<sup>43</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) (“GAO Report”).

<sup>44</sup> See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

<sup>45</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

<sup>46</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>47</sup> <https://datacoup.com/>

<sup>48</sup> <https://digi.me/what-is-digime/>

122. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>49</sup>

123. As a result of the Data Breach, Plaintiff’s and Class Members’ Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

124. At all relevant times, AGC knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

<sup>49</sup> *Medical I.D. Theft*, EFraudPrevention  
<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.>

125. The fraudulent activity resulting from the Data Breach may not come to light for years.

126. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

127. AGC was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than twenty thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

128. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

***Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary***

129. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the



Private Information for identity theft crimes –e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

130. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

131. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

132. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach.

### ***Loss Of Benefit Of The Bargain***

133. Furthermore, Defendant’s poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When submitting Private Information to Defendant under certain terms through a job application and/or onboarding paperwork, Plaintiff and other reasonable employees understood and expected that Defendant would properly safeguard and protect their Private Information, when in

fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received an employment position of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

***Plaintiff Richard Teague's Experience***

134. Plaintiff Richard Teague is a former AGC employee who worked at Defendant from approximately 2016 to 2019.

135. In the course of enrolling in employment with Defendant and as a condition of employment, he was required to supply Defendant with his Private Information, including but not limited to: his name, Social Security number, and other sensitive information.

136. At the time of the Data Breach—December 12, 2023 through December 17, 2023—AGC retained Plaintiff's Private Information in its system.

137. Plaintiff Teague is very careful about sharing his sensitive Private Information. Mr. Teague stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

138. Plaintiff Teague received the Notice Letter, by U.S. mail, directly from Defendant, dated February 12, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, driver's license number,

financial account information associated with direct deposit, passport, payment card number, company network login credentials, and limited health insurance plan enrollment information for current and former health insurance plan participants.

139. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to “be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity[,]”<sup>50</sup> Plaintiff Teague made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach and signing up for the credit monitoring and identity theft protection services offered by Defendant. Plaintiff Teague has spent approximately 50 hours thus far dealing with the Data Breach—valuable time Plaintiff Teague otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

140. Plaintiff Teague suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit

---

<sup>50</sup> Notice Letter.

of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

141. The Data Breach has caused Plaintiff Teague to suffer fear, anxiety, and stress, which has been compounded by the fact that AGC has still not fully informed him of key details about the Data Breach's occurrence.

142. As a result of the Data Breach, Plaintiff Teague anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Teague is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

143. Plaintiff Teague has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

## **CLASS ALLEGATIONS**

144. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

145. The Class that Plaintiff seek to represent is defined as follows:

### **Nationwide Class**

All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in February 2024 (the “Class”).

146. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

147. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

148. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 20,000

individuals were impacted in the Data Breach.<sup>51</sup> The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

149. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;

---

<sup>51</sup> <https://apps.web.maine.gov/online/aeviewer/ME/40/2f090dbf-dda8-44b0-90f3-2098bfce9f68.shtml>

- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

150. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to

virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

151. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

152. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

153. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient



adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

154. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

155. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

156. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

157. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

158. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

159. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;

- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard employee Private Information; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

## **CAUSES OF ACTION**

### **COUNT I**

#### **Negligence**

#### **(On Behalf of Plaintiff and the Class)**

160. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 159 above as if fully set forth herein.

161. Defendant required Plaintiff and Class Members to submit non-public Private Information as a condition of employment or as a condition of receiving employee benefits.

162. Plaintiff and the Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information.

163. Defendant had a duty to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members.

164. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

165. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

166. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits

“unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

167. Defendant’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

168. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members’ Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members’ Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members’ Private Information; and
- e. Failing to detect in a timely manner that Class Members’ Private

Information had been compromised.

169. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

170. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

171. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

172. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for

unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

173. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

174. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT II**  
**Negligence *Per Se***  
**(On Behalf of Plaintiff and the Class)**

175. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 159 above as if fully set forth herein.

176. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

177. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate

computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

178. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

179. Plaintiff and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

180. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

181. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendant knew or should have known that they failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

182. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.



**COUNT III**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiff and the Class)**

183. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 159 above as if fully set forth herein.

184. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of their employment with Defendant.

185. Plaintiff and Class Members provided their labor and Private Information to Defendant in exchange for (among other things) Defendant's promise to protect their Private Information from unauthorized disclosure.

186. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

187. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

188. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the

Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

189. When Plaintiff and Class Members provided their Private Information to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

190. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

191. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

192. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of

its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

193. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

194. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

195. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

196. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

197. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

198. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT IV**

**Breach of Implied Covenant of Good Faith and Fair Dealing  
(On Behalf of Plaintiff and the Class)**

199. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 159 above as if fully set forth herein.

200. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached when there is no breach of a contract's actual and/or express terms.

201. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

202. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard employee Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

203. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

**COUNT V**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Class)**

204. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 159 above as if fully set forth herein.

205. This count is pleaded in the alternative to Plaintiff's breach of implied contract claim (Count III) and breach of implied covenant of good faith and fair dealing claim (Count IV) above.

206. Plaintiff and Class Members conferred a monetary benefit to Defendant in the form of providing labor to Defendant as well as the provision of their Private Information, which Defendant would be unable to engage in its regular course of business without.

207. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant and they accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of Private Information to Defendant from Plaintiff and Class Members is an integral part of Defendant's business. Without collecting and maintaining Plaintiff's and Class Members' Private Information, Defendant would be perform its services.

208. Defendant was supposed to use some of the monetary benefit provided to it by Plaintiff and Class Members to secure the Private Information belonging to

Plaintiff and Class Members by paying for costs of adequate data management and security.

209. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement necessary security measures to protect the Private Information of Plaintiff and Class Members.

210. Defendant gained access to the Plaintiff's and Class Members' Private Information through inequitable means because Defendant failed to disclose that it used inadequate security measures.

211. Plaintiff and Class Members were unaware of the inadequate security measures and would not have entrusted their Private Information to Defendant had they known of the inadequate security measures.

212. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

213. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the

actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

214. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

215. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds from the monetary benefit that it unjustly received from them.

**COUNT VI**  
**Recovery of Expenses of Litigation, O.C.G.A. § 13-6-11**  
**(On Behalf of Plaintiff and the Class)**

216. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 159.

217. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in

bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense.”

218. Defendant through its actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused the Plaintiff and the Class Members unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

219. The Plaintiff and the Class Members request that their claim for recovery of expenses of litigation and attorneys’ fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys’ fees pursuant to O.C.G.A. § 13-6-11.

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

- A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;



- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.
  - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless AGC can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
  - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
  - v. prohibiting Defendant from maintaining the Private Information

- of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
  - vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
  - viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
  - ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
  - x. requiring Defendant to conduct regular database scanning and securing checks;
  - xi. requiring Defendant to establish an information security training program that includes at least annual information security

training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether

monitoring tools are appropriately configured, tested, and updated;

- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
- xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses pursuant to O.C.G.A. § 13-6-11 and as otherwise allowed by law;

- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: February 23, 2024

Respectfully Submitted,

By: /s/ MaryBeth V. Gibson

MaryBeth V. Gibson

GA Bar No. 725843

**Gibson Consumer Law Group, LLC**

4729 Roswell Road

Suite 208-108

Atlanta, GA 30342

Telephone: (678) 642-2503

[marybeth@gibsonconsumerlawgroup.com](mailto:marybeth@gibsonconsumerlawgroup.com)

John J. Nelson\*

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN, PLLC**

280 S. Beverly Drive

Beverly Hills, CA 90212

Telephone: (858) 209-6941

Email: [jnelson@milberg.com](mailto:jnelson@milberg.com)

*Attorneys for Plaintiff and  
Proposed Class Counsel*

*\*Pro Hac Vice Application Forthcoming*

**LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE**

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14-point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: February 23, 2024

/s/ MaryBeth V. Gibson  
MaryBeth V. Gibson